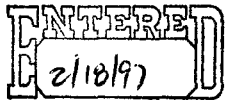
#38



KEY ESCROW WORKING GROUP

COMMENTS ON Bureau of Export Administration
Interim Rule on Encryption

February 13, 1997

Nancy Crowe

Regulatory Policy Division

Bureau of Export Administration

Department of Commerce

14th Street and Pennsylvania Avenue, N.W.

Room 2705

Washington, D.C. 20230

Re: Comments on *Bureau of Export Administration Interim Rule on Encryption Exports*, Issued December 30, 1996

Dear Ms. Crowe:

The Key Escrow Working Group of the Information Security Committee, Section of Science and Technology, American Bar Association, offers the following observations, comments, and suggestions to the *Bureau of Export Administration Interim Rule on Encryption Exports*. Please note that the views expressed herein have not been approved by the Information Security Committee, the Council of the Section of Science and Technology, the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the position of the American Bar Association.

The Information Security Committee is working to create a legally sound and technically viable framework for the emerging global public key infrastructure. The Information Security Committee consists of lawyers and technologists representing state and federal agencies, private industry, and firms. It includes lawyers, barristers, notaries, and technologists from several countries in Europe and Asia. Among the ISC's accomplishments is the Digital Signature Guidelines, which were released in June 1996.

The Key Escrow Working Group (KEWG) of the Information Security Committee is engaged in the development of guidelines to support the commercial use of key escrow mechanisms. Consistent with these efforts, the KEWG undertook considerable discussion and debate in order to produce the following comments.

1. Changes to Consider in order to Facilitate Business

> "On October 1, 1996, the Administration announced a plan to make it easier for Americans to use stronger encryption products to protect their privacy, intellectual property and other valuable information. The plan envisions a worldwide key management infrastructure with the use of key escrow and key encryption items to promote electronic commerce and secure communications while protecting national security and public safety. To provide for a transition period for the development of this key management infrastructure, this rule permits the export and reexport of 56-bit key length DES or equivalent strength encryption items under the authority of a License Exception, if an exporter makes satisfactory commitments to build and/or market recoverable encryption items and to help build the supporting international infrastructure." (From Summary.)
>
> Comments on *Bureau of Export Administration Interim Rule on Encryption Exports*

Strong cryptography is essential to protect our telecommunications infrastructure. The above paragraph of the Interim Rule, however, hinders the sales of domestic vendors' cryptography products and may distort the development of a market for key recovery products. It is difficult for domestic vendors to compete with their foreign counterparts under the Interim Rule, because foreign vendors are able to offer cryptography products without the limitations proposed in the United States. Moreover, domestic vendors may be reluctant to make long term investments in exportable cryptography products that can be sold only for two years and must be subject to an export license renewal evaluation every six months. The Interim Rule will therefore erode the technological lead currently held by domestic cryptography vendors.

The proposed regulation may distort the market for key recovery products because the market has not demanded recovery products of the kind required by the interim rule. The most efficient market will arise from products demanded by companies that have engaged in long-term planning and risk assessment, rather than a design promoted by the Interim Rule in the short term. Consequently, the Interim Rule may pose an obstacle to the free market migrating toward the most efficient designs and best practices.

A more acceptable approach would allow the marketplace for strong cryptography to develop unfettered by restrictive regulation. Sufficient controls on markets are already assured by contract, existing legislation (including antitrust legislation), and other well-established legal principles.

The Bureau should at the very least coordinate the final *Rule* with recommendations 4 through 4.3 made by the National Research Council in its study of issues in cryptography and policy, CRISIS (1996). The NRC, which has studied the issue from a number of perspectives and over some length of time, recommends progressively relaxing -- though not eliminating -- export controls, making products providing up to 56-bit DES and similar commercial algorithms "easily exportable," streamlining the export process, and allowing approved companies to export stronger encryption products if the companies are "willing to provide access to decrypted information upon legally authorized request." A professed adherence of a BXA final *Rule* to NRC recommendations would offer cryptography vendors more certainty and comfort as they plan their embryonic businesses.

2. Changes to Consider for Reasons of International Relations

(a) "To determine eligibility, exporters must submit a classification request to BXA. Requests for one-time review of key escrow and key recovery encryption items will receive favorable consideration provided that, prior to the export or reexport, a key recovery agent satisfactory to BXA has been identified (refer to Supplement No. 5 to part 742) and.. . . " (From Background.)

Provision effect: to give BXA (and not market participants) ultimate authority over what entities are suitable for service as Key Recovery Agents.

A BXA requirement of advance recognition of the key recovery agent ("KRA") may not be an appropriate method of handling international relationships. The BXA should not have sole authority to recognize KRAs . The term "satisfactory to BXA" deserves elucidation.

Issues that require clarification include:

- Who would be parties to a bilateral agreement that would recognize a foreign KRA?
- The Interim Rule assumes that KRA information will be fixed over time. This assumption may not be sound. In contrast to the Interim Rule, both business partners and software must be flexible enough to adapt to a changing KRA environment. In this environment, particulars about foreign KRAs may change from the time of classification request until operation of the software.

(b) "Note: Use of key recovery agents located outside the U.S. is permitted if acceptable to BXA in consultation with the host government, as appropriate." (From Supplement No. 5 to Part 742--Key Escrow or Key Recovery Agent Criteria, Security Policies, and Key Escrow or Key Recovery Procedures.)

Provision effect: to remove from U.S.-based buyers and sellers the ability to negotiate a significant contractual element in the key recovery process.

The goal of encryption vendors is to allow the use of key recovery products internationally. As stated in the above provision of the Interim Rule, the ratification of an agreement between two governments will result in automatic reciprocal recognition of KRAs. Such reciprocity may implicate U.S. constitutional protections of U.S. citizens if foreign governments could access the keys of U.S. citizens simply by serving a request on their own local authorized legal authorities that would automatically be recognized in the United States. Foreign governments may then possibly have access to U.S. citizens' key-encrypted data with some level of participation of the federal government.

3. Changes to Consider for Reasons of Incompleteness in the *Interim Rule*

(a) "(1) The key(s) or other material/information required to decrypt ciphertext shall be accessible though a key recovery feature.
(2) The product's cryptographic functions shall be inoperable until the key(s) or other material/information required to decrypt ciphertext is recoverable

> by government officials under proper legal authority and without the cooperation or knowledge of the user.
> (3) The output of the product shall automatically include, in an accessible format and with a reasonable frequency, the identity of the key recovery agent(s) and information sufficient for the key recovery agent(s) to identify the key(s) or other material/information required to decrypt the ciphertext.
> (4) The product's key recovery functions shall allow access to the key(s) or other material/information needed to decrypt the ciphertext regardless of whether the product generated or received the ciphertext.
> (5) The product's key recovery functions shall allow for the recovery of all required decryption key(s) or other material/information required to decrypt ciphertext during a period of authorized access without requiring repeated presentations of access authorization to the key recovery agent(s)." (From Supplement No. 4 to Part 742--Key Escrow or Key Recovery Products Criteria Key Recovery Feature.)

Provision effect: to ease and speed information recoverability by authorized parties.

The list of features that must be exhibited by encryption products should be augmented to permit unrestricted movement and use of personalized encryption products across multiple international borders while the user is in transit. Encryption vendors will want to create a product that does not operate unless it meets all the requirements of BXA rules. To remain user-friendly, the encryption product itself must facilitate compliance with the laws of all countries in which end-users may operate the encryption software.

With portable encryption, a user may move through several nations whose governments may or may not have bilateral agreements with BXA as to KRAs and rules of encryption. The proposed language does not adequately address the portability of encryption products and practices. The *Rule* must be sufficiently explicit for vendors to offer products that will make it possible for encryption users who cross governmental borders to know how they can comply with the encryption regimes of the nations through which the user travels.

In addition, section (3) above should be amended to require that the identity of the KRA and all other information be inextricably linked to the encrypted text in such a manner as to make it impossible to decrypt the text if this information has been tampered with. (One of the flaws with Clipper was that it was possible to substitute

another LEAF field -- both without detection and without disabling the decryption process.)

(b) "III. Key Recovery Procedures
(1) Key recovery agents shall maintain the ability to make the key(s) or other material/information required to decrypt ciphertext available until notified otherwise by BXA. Key recovery agents shall make requested key(s) or other material/information required to decrypt ciphertext available, to the extent required by the request, within two hours from the time they receive a request from a government agency acting under appropriate legal authority.
(2) Key recovery agents shall maintain data regarding key recovery requests received, release of key(s) or other material/information required to decrypt ciphertext, database changes, system administration access, and dates of such events for purposes of audits by BXA.
(3) The key recovery agent must transfer all key recovery equipment, key(s) and/or other material/information required to decrypt ciphertext, key recovery database, and all administrative information necessary to its key recovery operations to another key recovery agent approved by the BXA in the event that: (a) The key recovery agent dissolves or otherwise terminates escrowing operations, or (b) BXA determines that there is a risk of such dissolution or termination, or (c) BXA determines that the key recovery agent is no longer suitable or trustworthy." (From Supplement No. 5 to Part 742--Key Escrow or Key Recovery Agent Criteria . . . Key Escrow or Key Recovery Procedures.)

Provision effect: to identify appropriate key recovery activity in the event that encrypted data is to be accessed.

This list of duties that must be performed by the KRA to enable key recovery has a number of conspicuous omissions. Additional sections should address, at a minimum, three procedural safeguards. First, key recovery agent procedures should specify requirements and conditions that must be satisfied prior to a release of information to any requester. Second, key recovery agents must have a means of verifying that a request from appropriate legal authority is, indeed, a valid request. Verification measures might include confirming the time period, the name of the entity written in the warrant, and the type of information expected to be intercepted. When that verification is not possible or when there is asynchronicity, the key recovery agent's recourse to proper legal authorities should be made explicit. A third provision should

specify that KRAs can require that the key-encrypted material deposited with them must possess attributes that make it possible to narrowly search through the stored data/communications.

In addition to these topics for supplementary provisions, the Key Escrow Working Group recommends modifications to the first three sections. Section (1) leaves undefined the time frame for appropriate KRA retention of keys. What is a reasonable time? Furthermore, can the user ever request that keys be deleted? How are the identity and legal authority of the government agency to be confirmed? A two-hour compliance requirement provides insufficient time to challenge demands that a KRA might legitimately regard as dubious.

Section (3) borders on unconstitutionality for at least two reasons. First, requiring transfer of "all key recovery equipment," upon BXA's initiative and without due process, may be a taking. Second, language of subpart (b) that allows BXA officials to acquire all of a KRA's business equipment when it determines "there is a risk" that the KRA might dissolve or terminate operations appears on its face to be vague and overbroad.

In addition, the structure set out by this provision as a whole leaves a tremendous amount of uncertainty about the implications for domestic and international commerce if a particular KRA's authority or certificate is revoked, instantly leaving perhaps millions of users unable to communicate securely. What notice provisions will the final *Rule* implement to handle such occurrences?

(c) "I. Key Recovery Agent Requirements
(1)(a) A key recovery agent . . .
(b) Must certify that such individual(s) meet the requirements of the following paragraphs (b)(i) or (b)(ii). BXA reserves the right to determine at any time the suitability and trustworthiness of such individual(s). Evidence of an individual's suitability and trustworthiness shall include:
(i) Information indicating that the individual(s):
(A) Has no criminal convictions of any kind or pending criminal charges of any kind;

> (B) Has not breached fiduciary responsibilities (e.g., has not violated any surety or performance bonds); and.. . ." (From Supplement No. 4 to Part 742--Key Escrow or Key Recovery Products Criteria Key Recovery Feature.)

Provision effect: to give BXA ultimate authority over what persons are suitable for employment by Key Recovery Agents.

It is necessary to establish the parameters of an individual's "suitability" to act as a key recovery agent. The Interim Rule should specify both initial qualification and criteria of rejection or disqualification. The current language leaves room for capriciousness (and a resulting instability) in the determination process. Without a fully detailed clarification, businesses cannot know which KRAs they can rely on beyond the present moment. Does BXA propose to investigate every employee of domestic and foreign KRAs, and by what right or mechanism will BXA be able to force the removal of any unsuitable person(s)?

Section (B) above includes the criterion that KRAs must not have breached fiduciary responsibilities. Two concerns immediately present themselves. First, both the definition of a "fiduciary responsibility," and the standard to be used in measuring a breach of this responsibility, are entirely unclear. Second, any discussion of "fiduciary duty" leads naturally to a discussion of liability. The *Interim Rule* is mute on the nature of liability apportionment in key recovery procedures. It would be best to eliminate any mention of terms or rules that raise the necessity of discussing liability until the market has more fully developed. Otherwise a full and detailed framework for apportioning liability in the mishandling of keys is required in the final *Rule*.

Conclusion

The Key Escrow Working Group of the Information Security Committee of the Section of Science and Technology, American Bar Association respectfully requests that these suggestions to the BXA *Interim Rule on Encryption Exports* will be duly considered and acted upon in the final *Rule*.

Sincerely,

Key Escrow Working Group Co-Chairs

/s/ Dwight Olson

Dwight Olson

Emily Frye

Key Escrow Working Group
Information Security Committee
Section of Science and Technology
American Bar Association